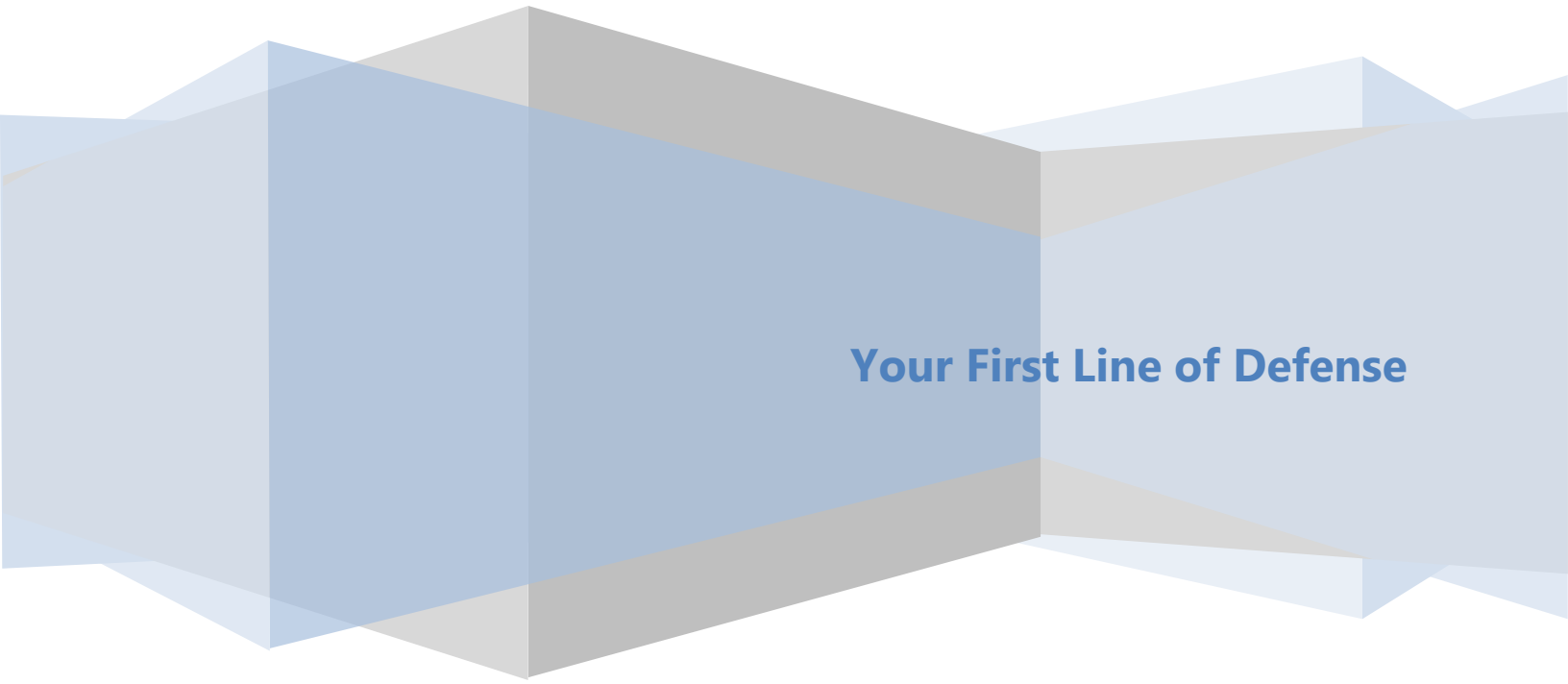
Infinity 2020 Perimeter Intrusion Detection System

User Guide: Network Application



Your First Line of Defense

Table of Contents

Section 1: Getting Started 2
Network Application: Browser Based 2
Launching the Application 3
Key GUI Features 4
Start System 5
Sidebar Menu 6
Weather Status Query 8
Alarm Queue 8
Zone Status 8
Zone Setup 8
Section 2: Site Alarm Reporting and User Interaction 9
Alarm Event Types 9
Zone Alarms 10
Processor Alarms 11
Acknowledging and Clearing Alarms 11
Managing Assignable Causes 15
Section 3: Working with System Parameters 16
Controller Card Configuration Settings 16
Transponder Card Configuration Settings 17
Configuring Zone Parameters 18
Scheduling Zone Status 23
Section 4: System Notes and Reporting 25
System Notes 25
Standard Graphical Reports 26
Alarm Event Occurrences by Zone 26
Alarm Event Occurences by Zone and Type 27
Alarm Frequency by Period and Type 27
Assignable Cause Report 28
System Status Changes by User and Period 28
Site Activity Report 29
Printing Site Activity Reports 30
Exporting Site Activity Reports 30

Section 1: Getting Started

Major points covered in this section:

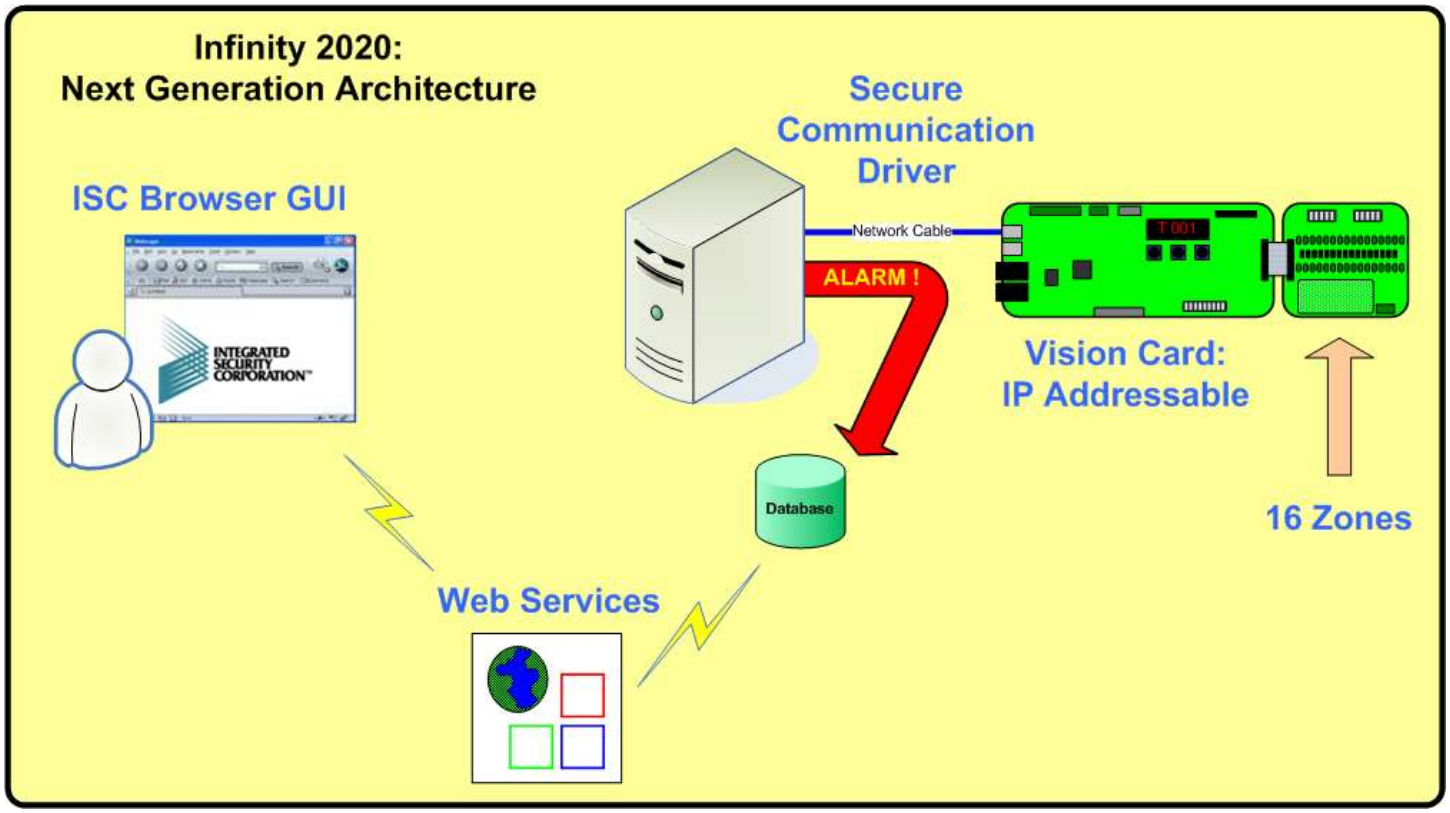
- ✓ Technology Overview
- ✓ Launching the Application
- ✓ Pertinent GUI Features

Next Generation Technology

Integrated Security Corporation (**ISC**) perimeter intrusion detection systems have been providing industry leading performance for over twenty years. The **Infinity 2020** set of next generation hardware and software leverages today's networked technology while maintaining the same performance, reliability, and trouble-free maintenance our customers have come to know and expect.

Network Application: Browser Based

The Internet Age has provided explosive growth and greater efficiency in all areas of our world. Devices can now be easily deployed within existing secure private networks and interrogated from any networked PC. The figure below provides an overview of the ISC's typical networked system configuration:

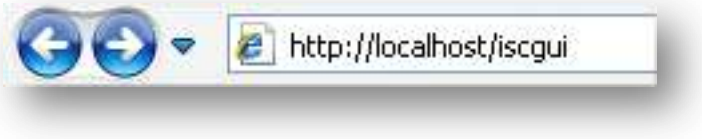


The **Vision Card** monitors up to 16 field mounted sensor cable inputs and reports alarm activity over **TCP/IP encrypted Ethernet** communication links (copper or fiber) to a network PC running the **Infinity 2020 Network Application**. The Vision Card can function as a **Controller** or a **Transponder**. The Controller periodically interrogates one or more transponders and passes any alarm events to the application. Transponders monitor **Sensor Line** activity to detect intrusions and pass them to the Controller. The Vision Card which is configured as the Controller also has an on-board Transponder. The application is comprised of several Windows based alarm services some of which write system activity to the **ISC database**. The site monitoring and control GUI is accomplished via a **web browser** providing clear situational awareness of the sites Perimeter Security through the **Web Services** interface. This web services interface will also provide an efficient standardized method to relay current perimeter security information to 3rd party integrators.

Launching the Application

Since **the Infinity 2020 Application** is browser based the first step in starting the application is to run Microsoft Internet Explorer (this is the only tested and approved web browser).

The application is served up on the local machine using **Internet Information Services** (**IIS**) and is accessed by typing http://localhost/iscgui in the address then depressing **ENTER**.



A Note on the Windows Computer Administrator Account:

A Microsoft Windows Computer Administrator account was created by ISC for the initial installation and current execution of this Network Application. Any changes to this account will disable the execution of the application. Site personnel log into this account by entering the password of "**infinity**".

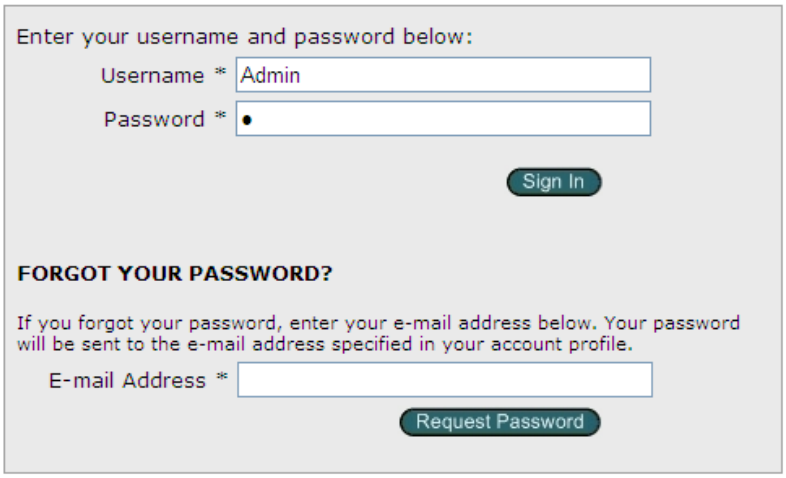
After the web page has loaded the user will be prompted to log in. Access to various features of the system is controlled by **User Roles**. There are 4 user roles: **Developer**, **Administrator**, **Supervisor**, and **User**. The various system functions accessible to each user role will be detailed later in this document. A default **Administrator** account is provided with the following login credentials:

Role: Administrator
Username: "**Admin**"
Password: "**a**"

Role: Supervisor
Username: "**super**"
Password: "**s**"

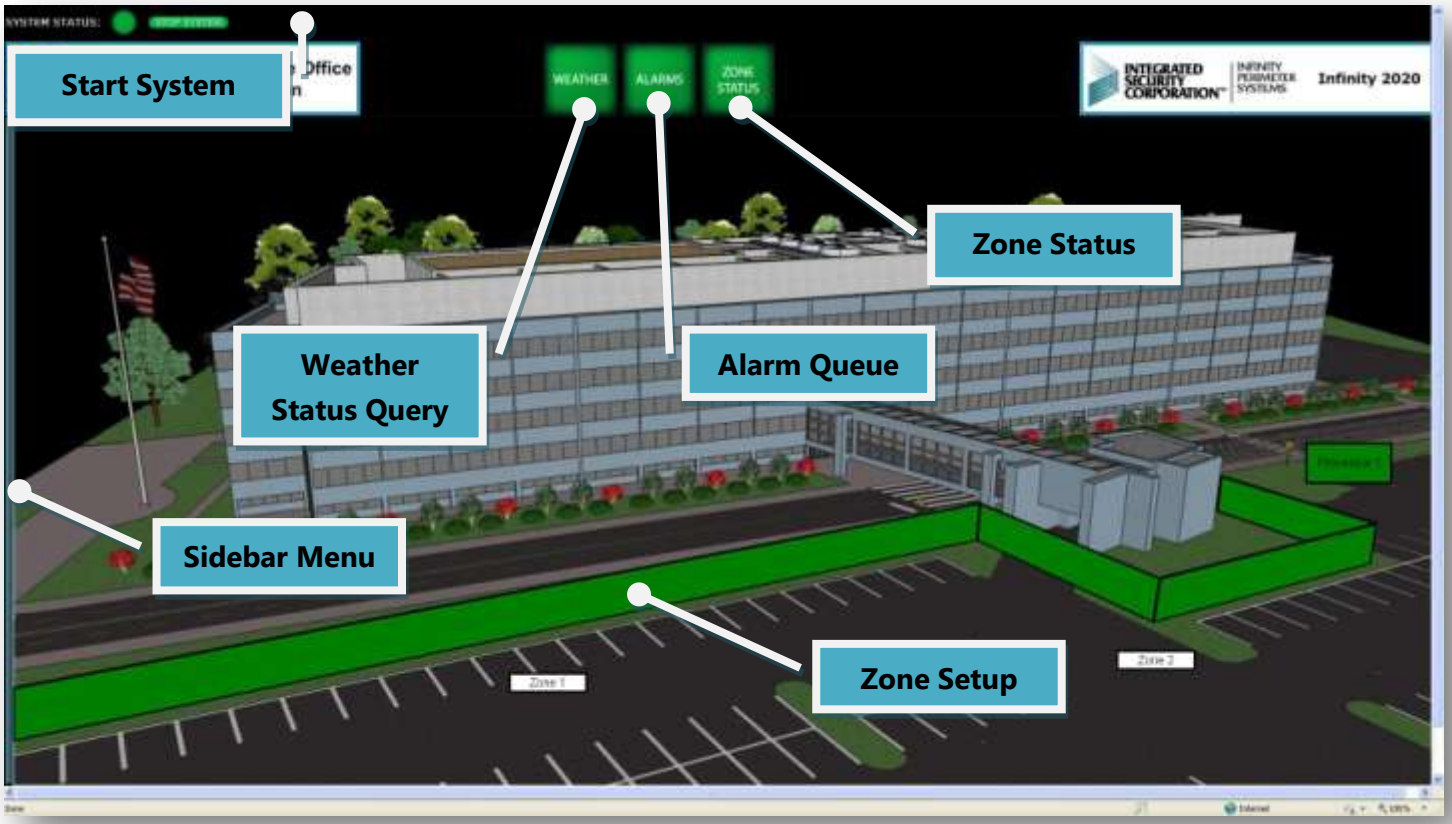
Role: General User
Username: "**user**"
Password: "**u**"

Log in to default Administrator account:


Enter your username and password below:
Username * Admin
Password *
Sign In
FORGOT YOUR PASSWORD?
If you forgot your password, enter your e-mail address below. Your password will be sent to the e-mail address specified in your account profile.
E-mail Address *
Request Password

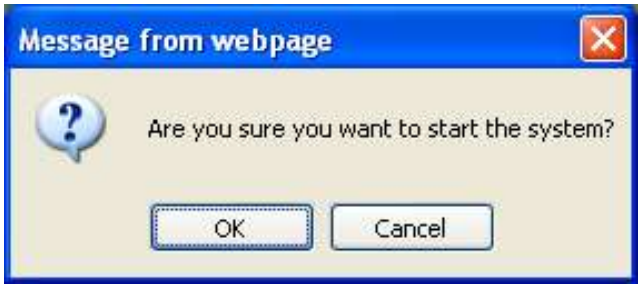
Key GUI Features

The **ISC Network Application** provides the site user clear, graphically based controls for straightforward system operation. System functions include changing **Infinity 2020 Perimeter Security System** parameters, responding to alarm events, managing user access, entering system notes, defining assignable causes, and querying the database for customized graphical and text based system activity reports. After successful login the main site graphics page will be loaded displaying the site graphics along and with its associated perimeter security zoning. The high level system controls are provided in the callouts below:

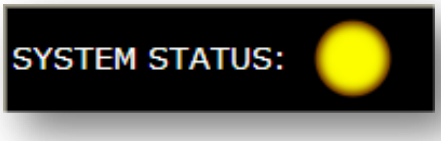


Start System

When the main site page is first loaded the System Status will be inactive as indicated by the red colored system activity icon. System initialization gets under way by a mouse click on the **Start System** button. When this occurs the application will prompt the user to ensure the system is to be started:



As the system settings are being downloaded to the Vision Card(s) the system activity icon becomes colored yellow:



When this process is complete the system is fully active allowing for full site monitoring and control as indicated by the green system status activity icon:

A Note on Stopping the System:

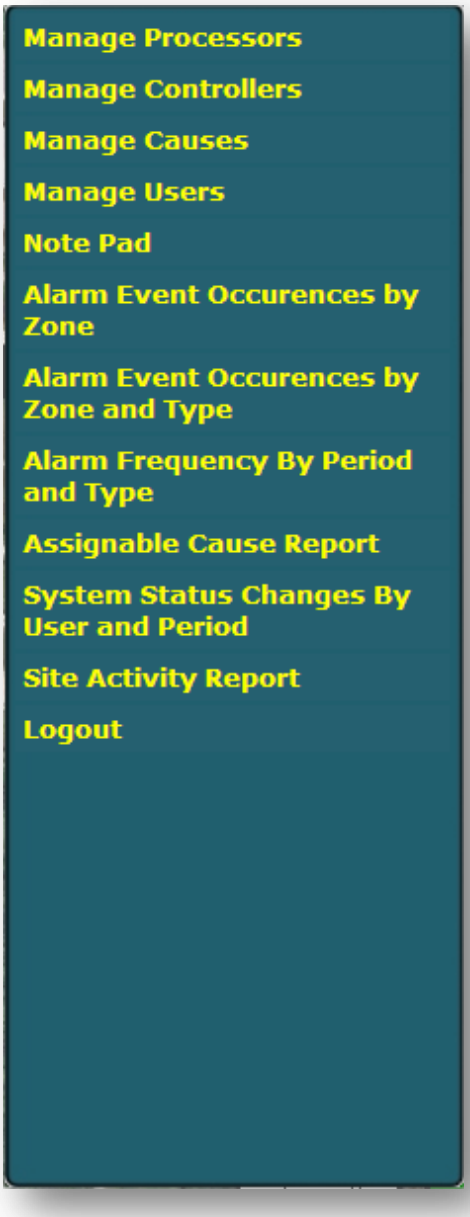
Closing the browser window alone in the typical manner does not stop the communications from the application to and from the Vision Card(s). In fact, if the browser window were closed without stopping the system and alarms occurred thereafter they would be reported to the user after re-login. Simply mouse click on the **Stop System** button to terminate communications with the system. Again the user will be prompted to ensure the system is to be stopped:

Sidebar Menu

The **Sidebar Menu** provides all users access to the various features of ISC's Perimeter Intrusion Detection System. The Sidebar Menu becomes visible by mouse clicking on the long vertical control bar on the left hand side of the screen. For full unobstructed site monitoring mouse click on the control bar again and the Sidebar Menu closes. The menu features available change depending on the user's defined **Role**. There are three site user roles: **Administrator**, **Supervisor**, and **User**. An ISC factory defined role, **Developer**, is provided for initial graphic site development and to modify application performance parameters. Only the Developer role has access to the **Manage Regions** and **Manage Application Configuration** features.

Note: it is extremely important that site administrators consult with the technical support team at ISC before making any Developer setup parameters. Doing so may result in severe system degradation.

This menu lists the features available to the administrator role:



A breakdown of systems features based on role is provided below:

Weather Status Query

Each **Vision Card** has the capability of receiving current wind speed and rain intensity compensation information from a field mounted **Weather Station**. Mouse down on the **Weather Status** button for an update of the current weather from one or more weather stations. All user roles have access to this feature.

Alarm Queue

The Alarm Queue provides a listing of the currently active alarms. The user can acknowledge and clear these alarms from the directly from the queue. All alarms are time and date stamped and tagged with the wind and rain information at the time of the alarm event. All user roles have access to this feature.

Zone Status

Each zone can be put in one of three arming states: **Secure**, **Access**, and **Disarm**. The secure state provides full alarm monitoring capability and it used by default for an active system. A disarmed zone is inactive and will not report any alarm events regardless of the activity level at that zone. There are also three types of Zone alarms which can be reported: **Alarm**, **Short**, and **Open**. "Alarm" is reported on a typical intrusion type disturbance (fence climb). For severe system tampering alarm events such as cutting the sensor line or tying it to an electrical ground "Open" or "Short" is respectively reported. When a zone is placed in the access state only "Short" or "Open" alarm events are reported. **Supervisor** and **Administrator** roles have access to this feature.

Zone Setup

All zone parameters can be easily viewed and configured via the zone graphic representation. Site personnel simply mouse click on the zone of interest to reveal it currents settings or change any of its parameters. **Zone Setup** parameters include Zone Status, Alarm Type, Period, Vibration Sensitivity, and Wind/Precipitation Compensation. The **Administrator** role has access to this feature.

Section 2: Site Alarm Reporting and User Interaction

Major points covered in this section:

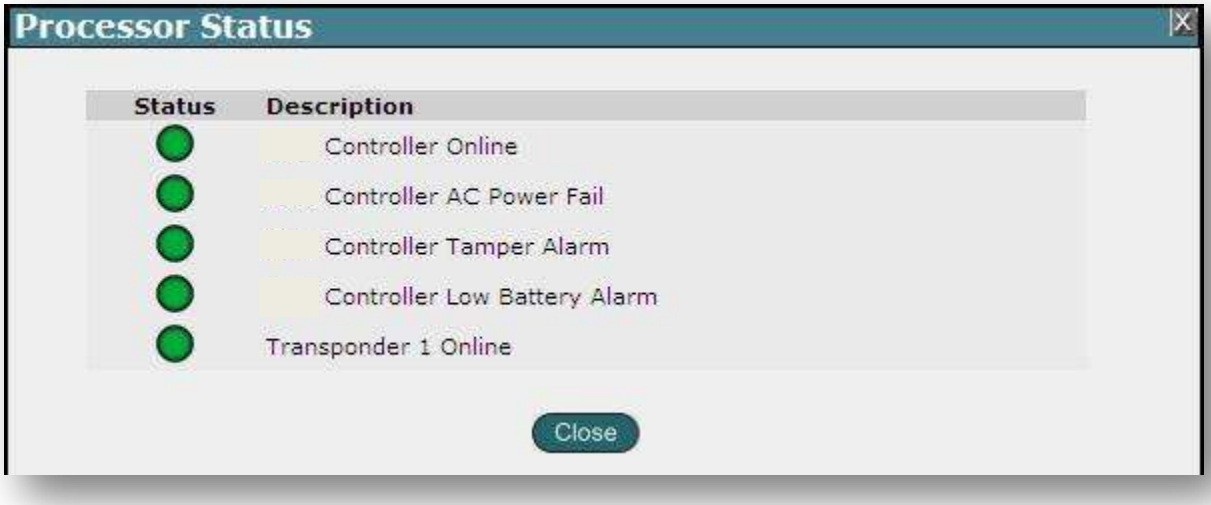
- ✓ GUI Presented Alarm Events
- ✓ Acknowledgement and Clearing of Alarms
- ✓ Managing Causes

GUI Alarm Events

Alarm Event Types

There are 2 categories of alarm events: **Processor** and **Zone**. Zone alarms represent those related to fence line intrusions and can be reported as Alarm, Short, or Open as described earlier. Processor type alarms relate to component issues found in enclosure mounted hardware. For instance, unauthorized entrance into an enclosure is detected via a **Tamper Switch** and reported as a **Tamper Alarm**. Other types of processor alarms include communication issues, **Controller and Transponder(s) Offline**, as well as, **AC Power Fail**, and **Low Battery** related to processor power issues. Mouse clicking on the rectangular processor icon provides the current status of that processor:

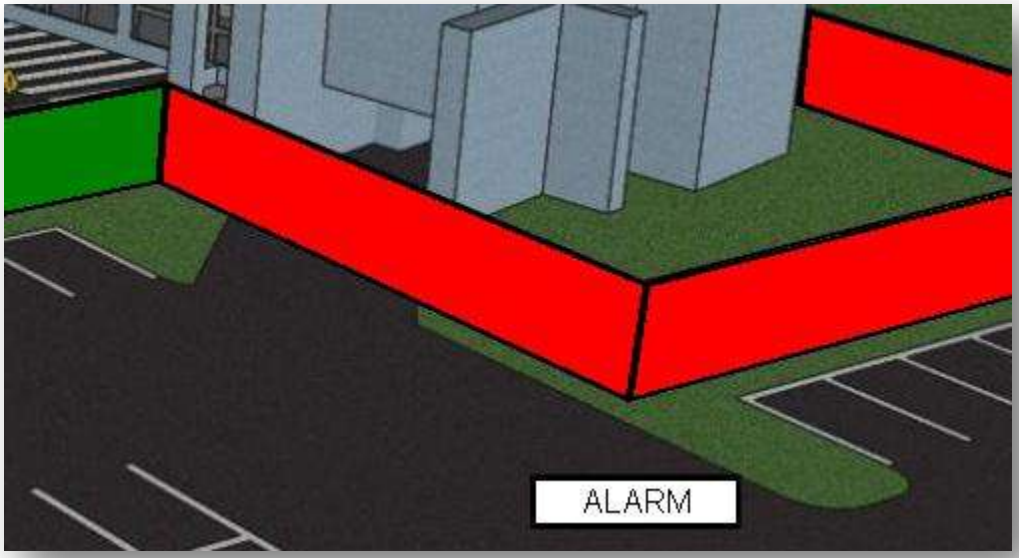
Current Status of Processor 1:



Zone Alarms

When any alarm event occurs the Alarm Queue button flashes red to green alerting the user of an active system alarm:

An audio message also accompanies all alarm events. In the case of a zone alarm the audio message of **"Alarm, Perimeter Fence"** is played, until the alarm is **acknowledged**. The zone graphic for that particular zone in alarm will also flash from red to green until acknowledged. Here **Zone 2** is in **Alarm**:



By mouse clicking on the Alarm Queue button the user can see the additional date/time stamp and weather information which further details the **Zone 2** Alarm Event.

Processor Alarms

Processor alarms report in the same manner as a zone alarm providing both a visual and audio alert. Here the **Processor P1** has an alarm indicated by the red to green flashing processor icon:

Mouse clicking on the processor icon reveals the particular type of processor alarm – here a **Transponder 1 Communication Notice Alarm**:

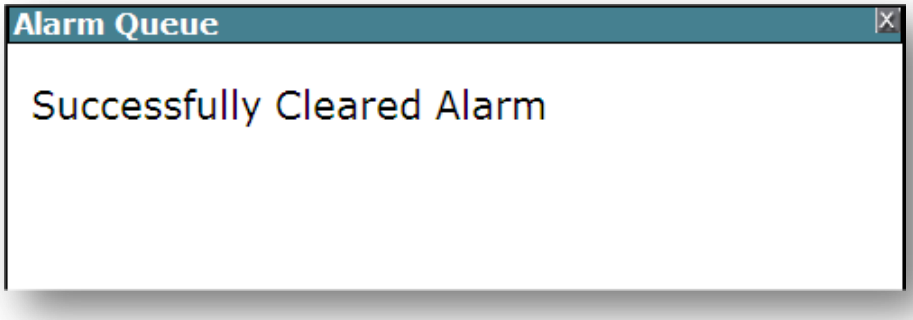
Again more details on this alarm can be found in the alarm queue:

Acknowledging and Clearing Alarms

Acknowledging alarms is graphically driven with the user mouse clicking either on the flashing zone/icon or the Ack/Clear link provided next to the alarm in the queue. Once acknowledged the flashing states change from red and green to **yellow and green** and the audio associated with that alarm is **silenced**.
Here the **Zone 2** alarm has been acknowledged:

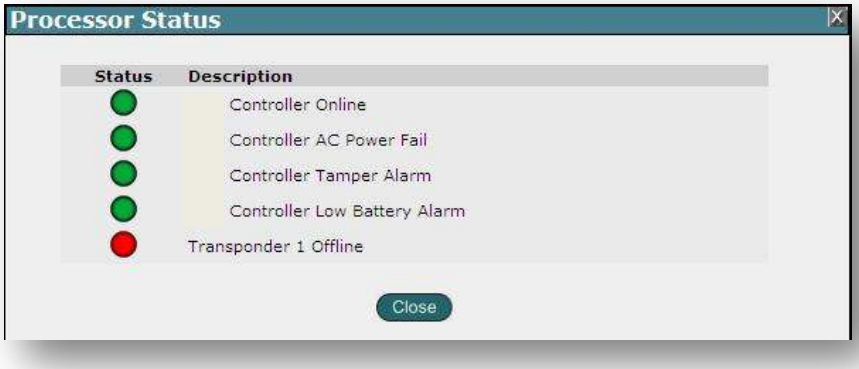
Once the source of the zone disturbance has been investigated and determined the user selects the assignable cause in the pull-down, and then simply mouse clicks on the **Clear** button. Note that the application will not allow a clear action without an assignable cause selection. The illustration below shows the application in the process of clearing the **Zone 2 alarm** having given **Testing** as the assignable cause.

Finally, the application posts that the alarm was successfully cleared.



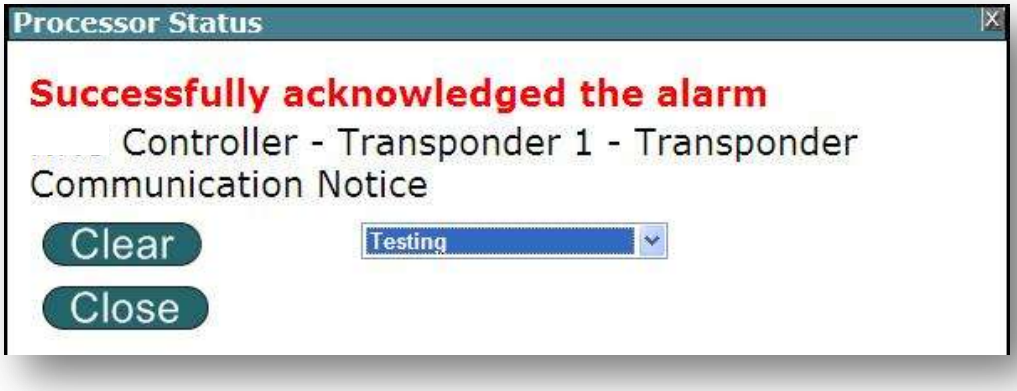
The process for acknowledging and clearing processor type alarms operates in the same manner. Here the West Processor has Transponder AC Power Fail alarm event. Here again the Processor icon and Alarm queue button flash from red to green indicator the presence of a processor type alarm:

An audio message also alerts personnel: **"Transponder Communication Notice."** The site user then mouse clicks on the Processor icon which confirms the presence of the Transponder Communication Notice.



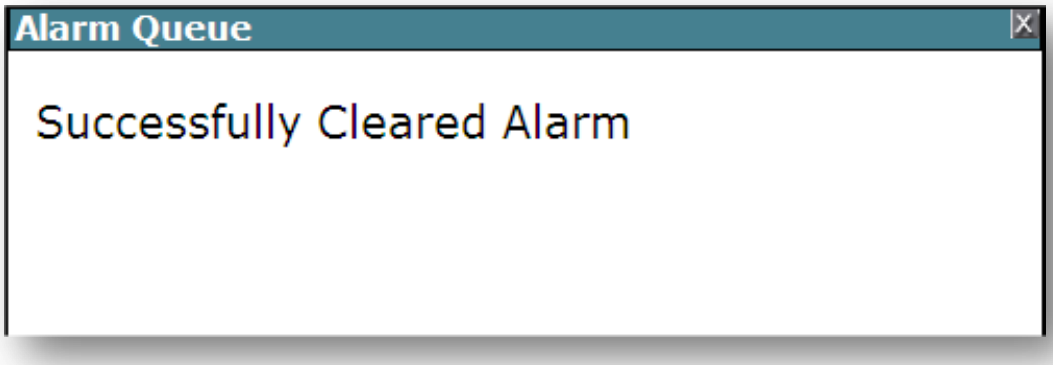
The alarm is acknowledged by mouse clicking on the red button icon next to Transponder 1 Offline description. At this point the audio message has been silenced the issue can be investigated:

Once the assignable cause has been determined the user simply selects it from the pull-down and selects **Clear**:



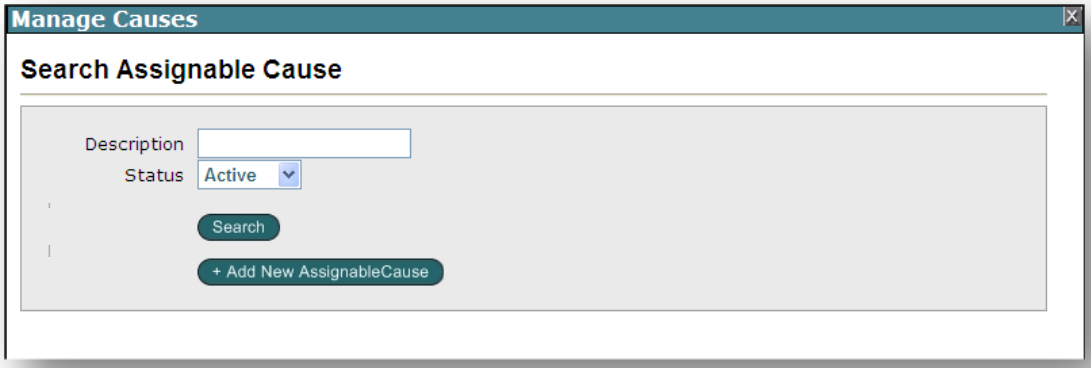
The clearing of processor type alarms takes longer than zone alarms especially on larger systems. This is due to the fact that approximately 144 parameters per card are queried and verified against the application settings to ensure parameter integrity.

Finally, the Clearing is confirmed:

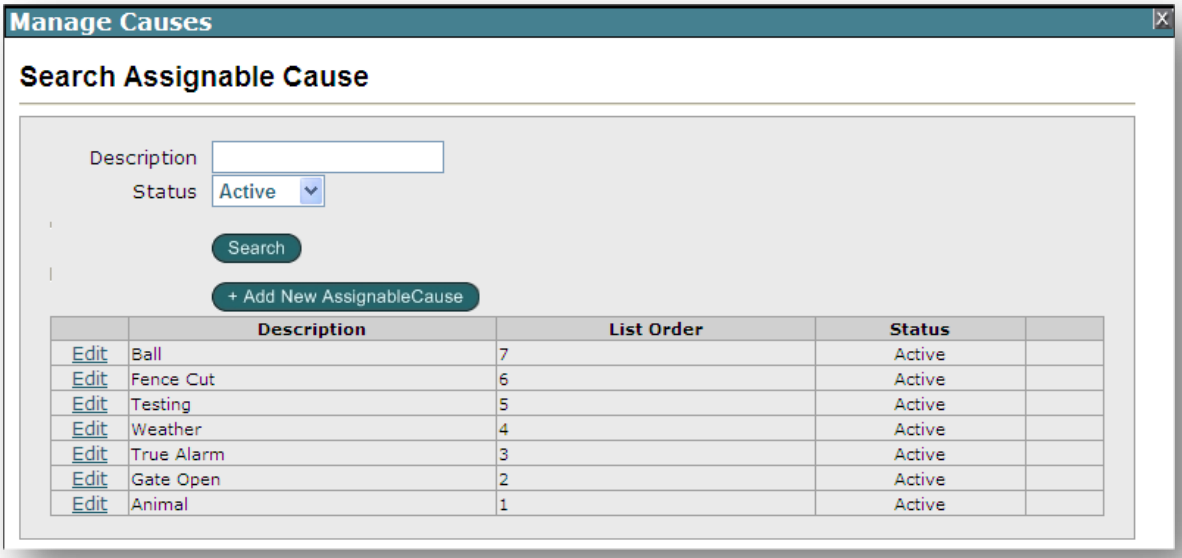


Managing Assignable Causes

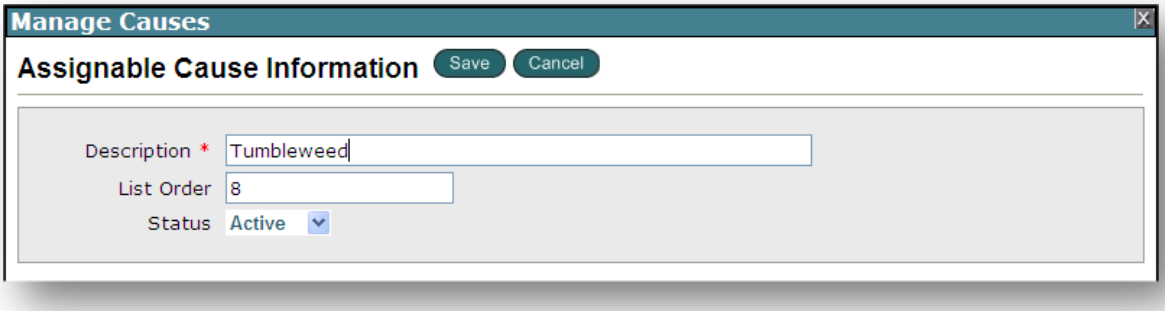
Various customers and sites may need to add assignable causes to meet their particular needs. This requires an administrator type role to be logged in. Selecting the **Manage Causes** item in the sidebar reveals the **Search Assignable Cause** page:



Selecting **Search** provides the current active listing of assignable causes and their listing order:



To add "Tumbleweed" select **+ Add New Assignable Cause** then enter this cause and the Listing Order:



Note that the user can inactivate current assignable causes which may not be relevant any longer via the **Status** selection.

Section 3: Working with System Parameters

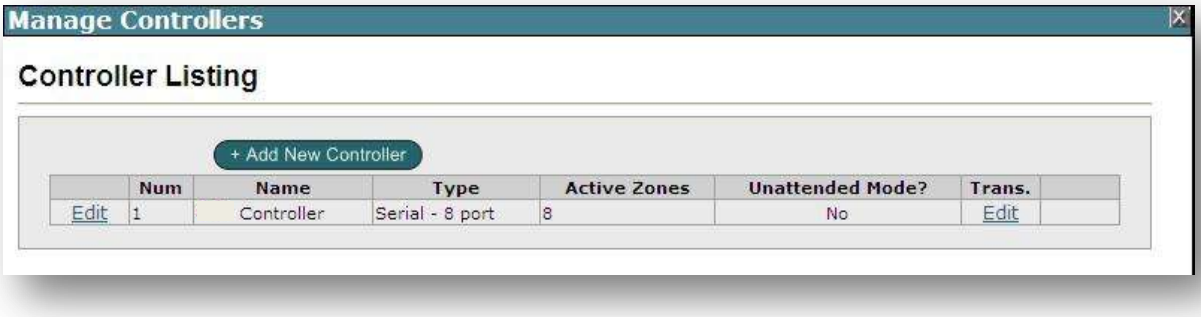
Major points covered in this section:

- ✓ Vision Card Configuration Settings
- ✓ Understanding and Changing Zone Parameters
- ✓ Creating Scheduled Zone Status Events

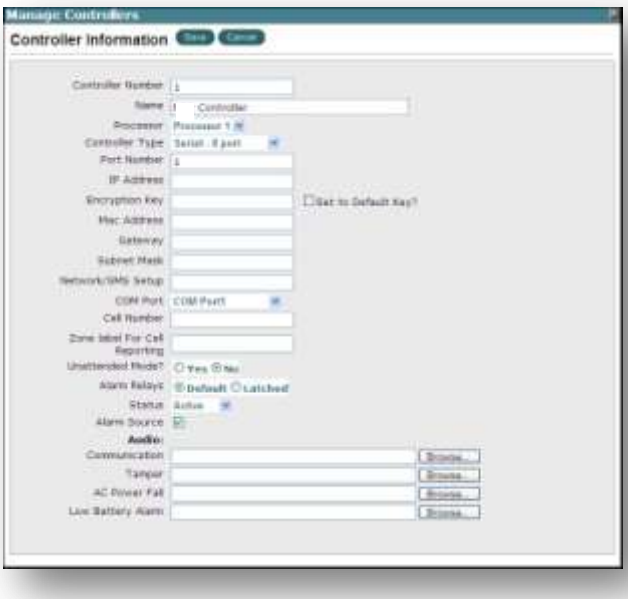
Vision Card Parameters

Controller Card Configuration Settings

In most applications **ISC** will design, configure, and test all final hardware parameters for the site. It may be helpful to know where the settings are for future reference. Key hardware setup information can be found under the **Manage Controllers** option under the sidebar menu. Select Edit on the left hand side to view the Controller setup parameters:



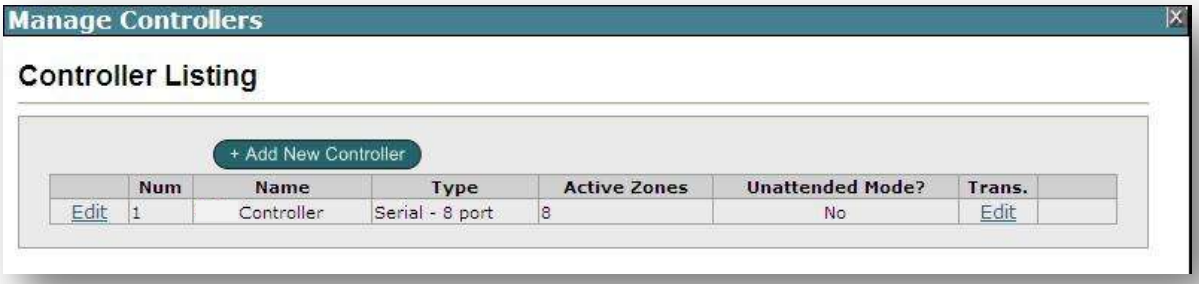
Key parameters that the application uses include: **Controller Number**, **Processor**, **Controller Type**, **Port Number**, **COM Port**, **Unattended Mode**, **Status**, **Alarm Source**, and **Audio**. The balance of the fields is for informational purposes only:



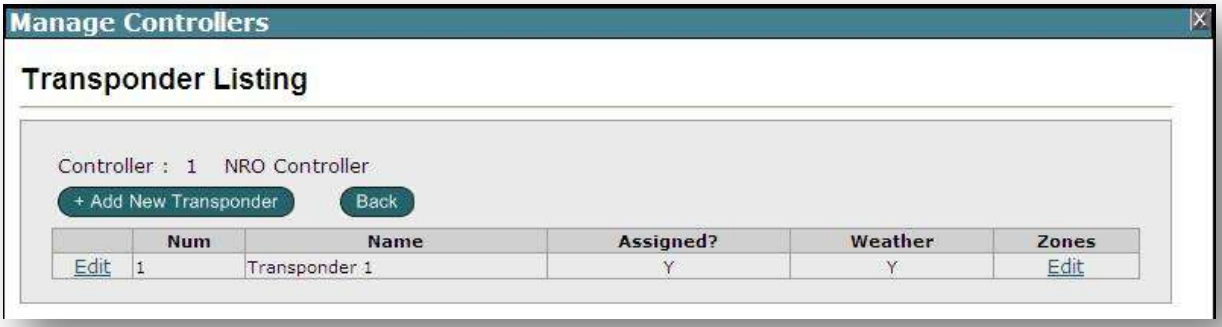
It is highly recommended that these parameters not be altered in any way without first consulting with the technical support team at ISC. Doing so may cause permanent connectivity issues from the application to the Vision Card thereby essentially disabling the system.

Transponder Card Configuration Settings

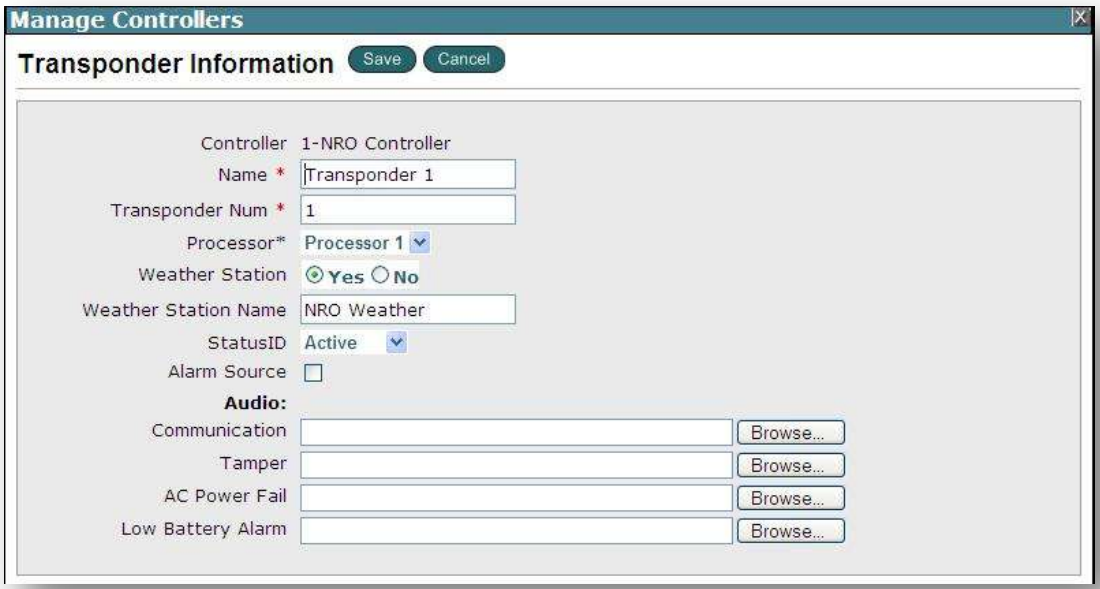
To view the setup parameters of Transponders select Edit located under the Transponder heading:



After this selection has been made the sites **Transponder Listing** will become available:



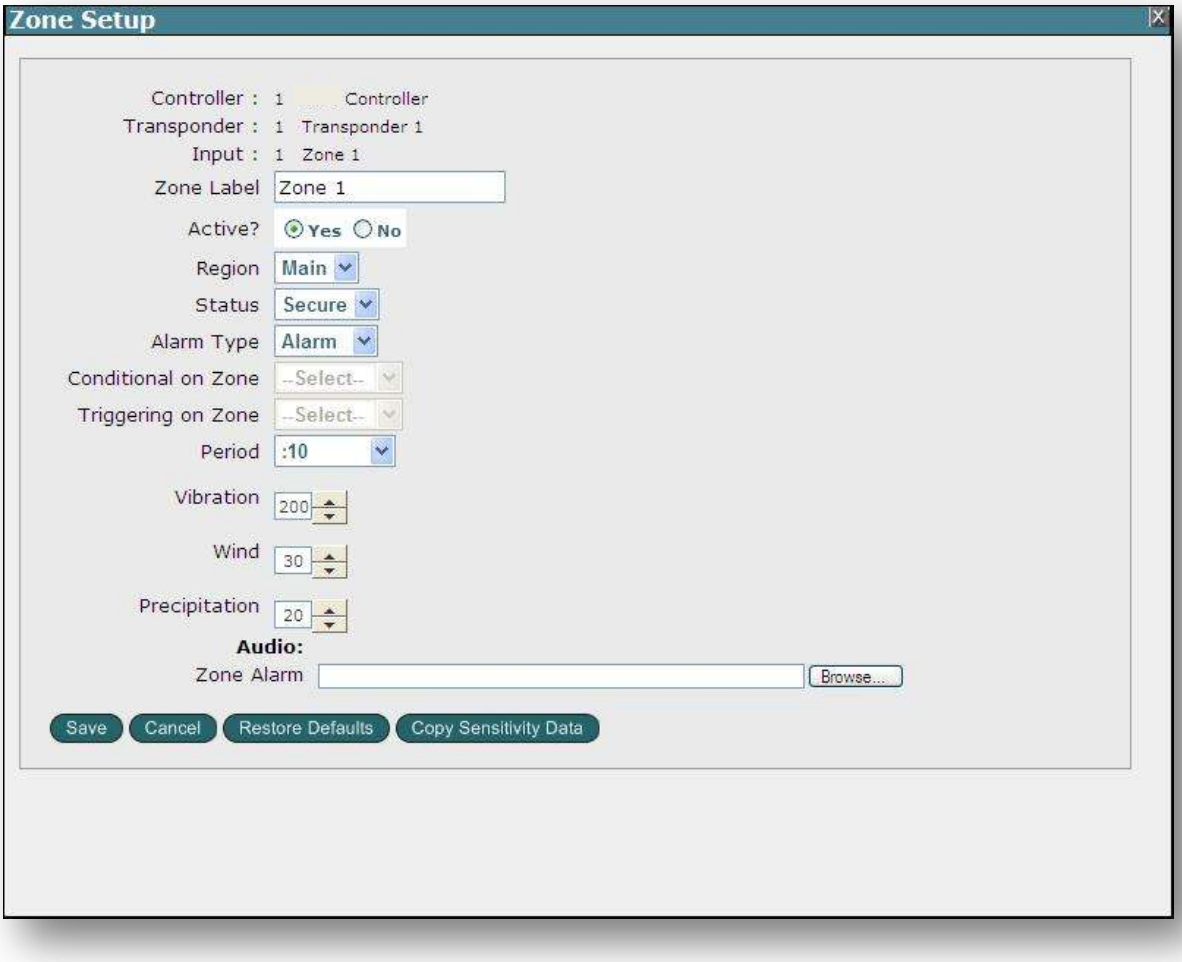
Select Edit on the left hand side of the Transponder of interest to view its current setup parameters:



All Transponder parameters listed are used by the application and should not be altered without factory support.

Configuring Zone Parameters

Changes to zone parameters can be accomplished via the GUI or the Sidebar Menu. Since the GUI is easier to relate to and more direct this method will be detailed first. All Zone Parameters can be found in the Zone Setup Window. To view these parameters you must be logged in with an Administrator Role. Simply mouse click on the graphical zone of interest (here **Zone 1**) to view the current settings:



The following is a brief description of the Zone Parameters and typical settings:

Controller:

Controller number and name

Transponder:

Transponder number and name

Input:

Vision card input number and name

Zone Label:

Zone name

Active:

Default setting: Yes - if made inactive Zone Alarm relay and Vision Card alarm messages are disabled

Region:

GUI Region Zone alarm reports to – configured by ISC personnel

Status:

The default setting is **Secure**. In this state all alarm conditions are reported. Conversely, when a particular zone is put in the **Disarm** state reporting of all alarms conditions is suppressed. The **Access** state is provided to suppress the reporting of the **Zone Alarms,** but allows **Zone Open** and **Zone Short** alarm types to be reported. Site personnel can use this feature short term for authorized gate activity as a way to minimize nuisance alarms - with the advantage of knowing if any tampering occurs by a physical cut in the sensor line or tying the sensor line to an electrical ground.

Alarm Type:

ALARM – With the **Alarm** type, any alarm condition in that zone will cause the system to report that an alarm has occurred. This is the default setting and would be used for the majority of the perimeter fence. The **Period** setting designates how long (in seconds) the **Open** or **Short Alarm** condition has to be active before it is reported.

EVENT – In the **Event** type, a condition that would ordinarily create an alarm is recorded, but does not produce an audio or visual indication at the GUI. For instance, a gate which is used for authorized access can be set as an Event zone. The **Site Activity Report** still maintains a record of every authorized access, along with the date and time that it occurred. From a hardware standpoint the zone relay outputs still maintain the operation of an Alarm type. The **Remote Event** (Revent) alarm type acts similarly, but does not allow the alarm relay to energize if the Conditional zone is active. Typical cases are **Cond/Event**, **Rcond/Event**, **Rcond/Revent**.

CONDITIONAL – The **Conditional** type is used for zones which are normally in an alarm state, but may be accessed without alarm if an adjacent zone has experienced authorized access. Most often, conditional zones would be used on either side of a gate to prevent the vibrations set up by the opening and closing of the gate from creating an alarm. Disturbance of the fence at any other time would produce an alarm. When the Conditional type is selected the **Conditional On Zone** becomes active for zone selection. Typical uses are **Conditional/Alarm** and **Conditional/Event** pairs. The **Remote Cond** (Rcond) alarm type acts similarly, but does not allow the alarm relay to energize if the Conditional Event or Revent is active.

DUAL – The **Dual** alarm type is an alarm condition that would require two zones to be in alarm within a software programmable time period before an alarm is reported to site personnel. An application of this would be the use of an interior microwave and an ISC perimeter fence sensor requiring both to be in alarm within a ten second window in order to report an alarm at the GUI.

TRIG - The Trigger alarm type is used in conjunction with the Dual alarm type to act as the trigger zone that must be alarmed before the "Dual" zone, to generate an alarm condition at the host. For example, Zone 1 is set to a Dual type, triggering on Zone 2 with a period of 10 seconds. That is, if both Zone 1 and Zone 2 are in an alarm condition within 10 seconds a Zone 1 alarm is reported.

Period:

The Period setting designates how long (in 10 second increments) the Open or Short Alarm condition has to be active before it is reported:

Vibration Sensitivity:

Assigns the Vibration Sensitivity level for a zone and ranges from 1 – 200 where 200 is the highest sensitivity level. Typical levels are 185 -190, but vary depending on fence type and site conditions.

Wind Sensitivity:

Assigns the Wind Sensitivity level for a zone and ranges from 1 – 100 where 100 represents the highest level of compensation. Typical levels are 15-20, but vary depending on site conditions.

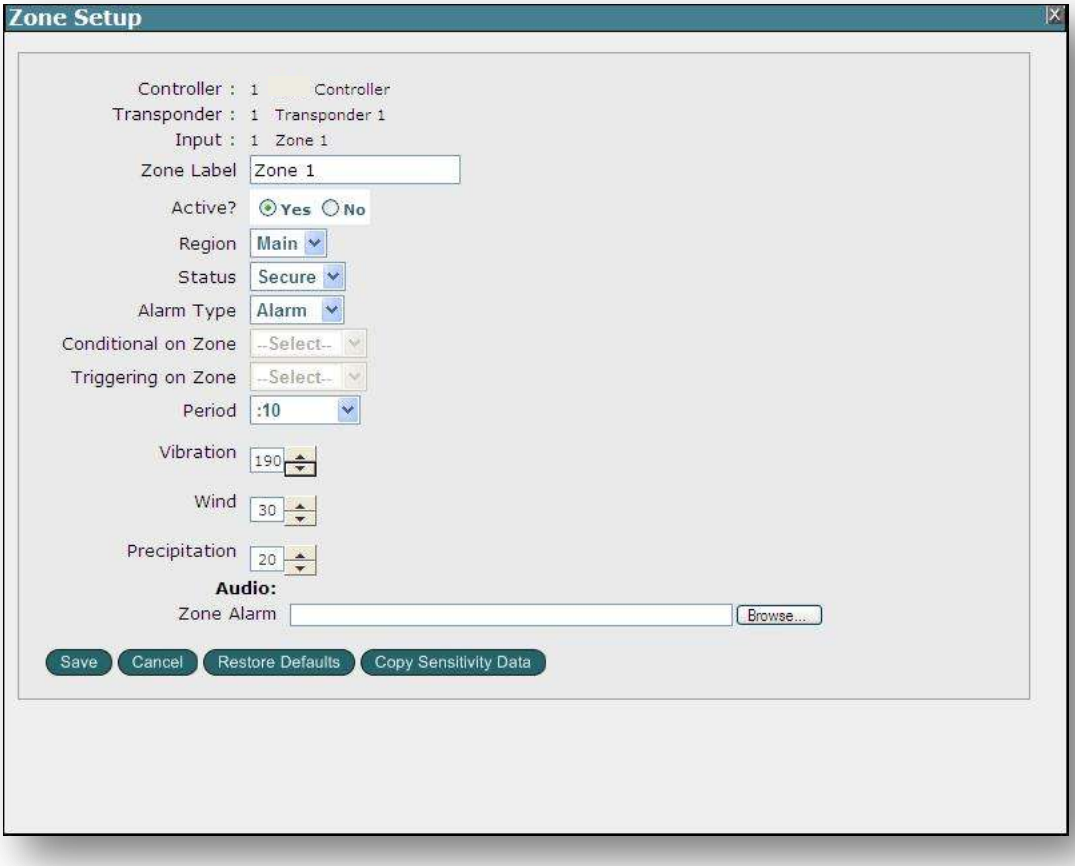
Precipitation Sensitivity:

Assigns the Precipitation Sensitivity level for a zone and ranges from 1 – 100 where 100 offers the highest level of compensation. Typical levels are 10-25, but vary depending on site conditions.

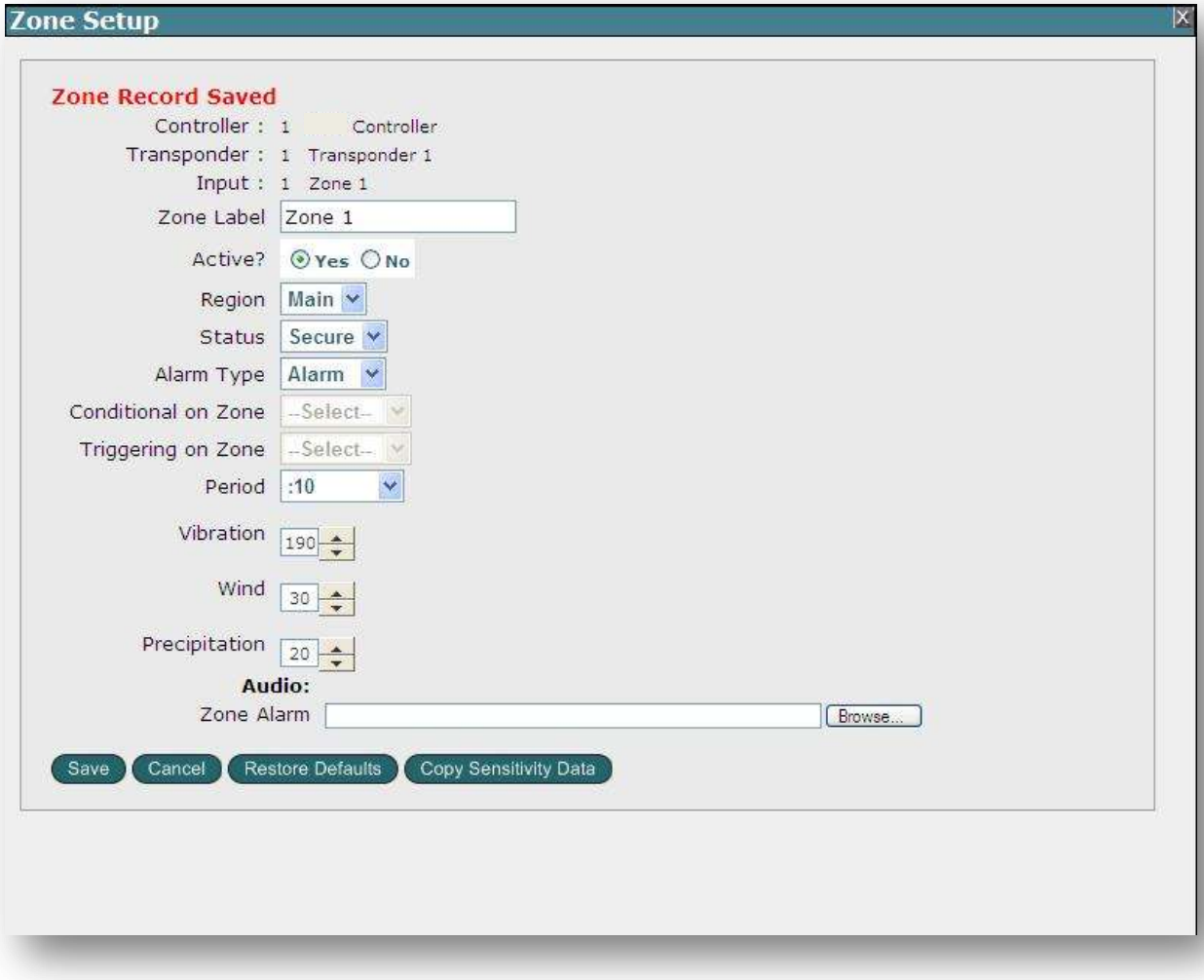
Audio:

Allows for customized audio notifications at each zone

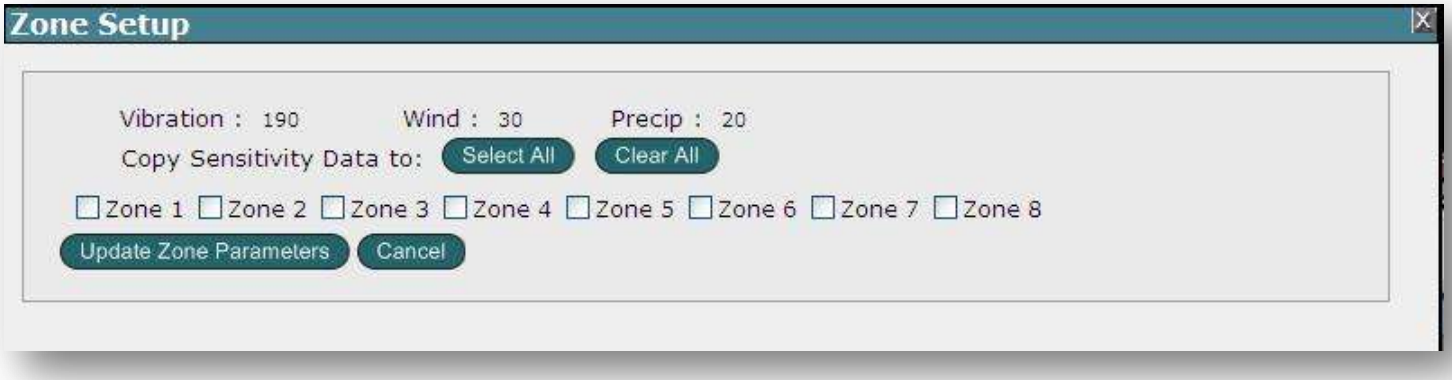
As an example, the **Vibration Sensitivity** level for **Zone 1** will be modified. Locate the Vibration Sensitivity control and change the value to 190. A **Save** action is required on any change so that the new value(s) are sent to the hardware and verified. Select Save to send the updated settings to the hardware:



Confirmation of the update is presented to the user with the response of **Zone Record Saved**:

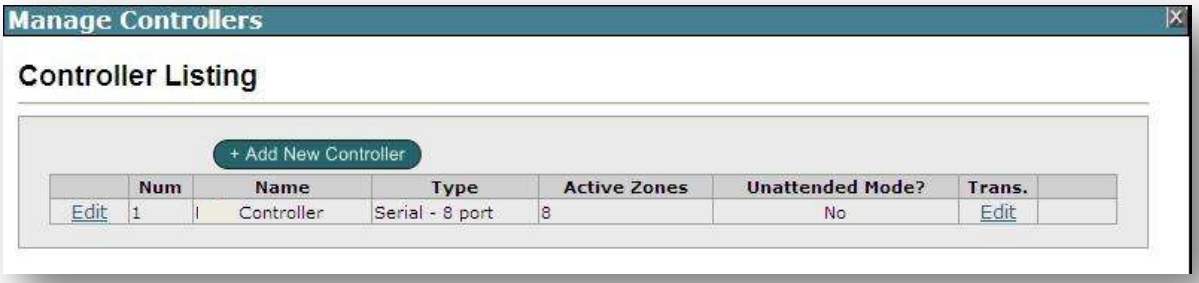


When the same Vibration, Wind, and Precipitation sensitivity changes are required across multiple zones the **Copy Sensitivity Data** can be quite helpful:

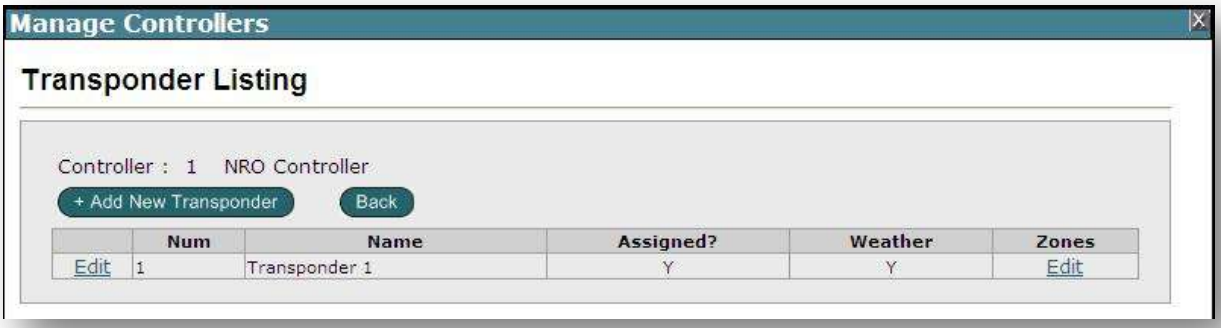


Select the zones which the new sensitivities will be applied then execute by selecting **Update Zone Parameters**. Note that **Select All** and **Clear All** are available for batch processing.

To view or edit zone setup parameters via the Sidebar Menu select **Manage Controllers** to display the **Controllers Listing** page then select Edit under the **Transponder** heading:

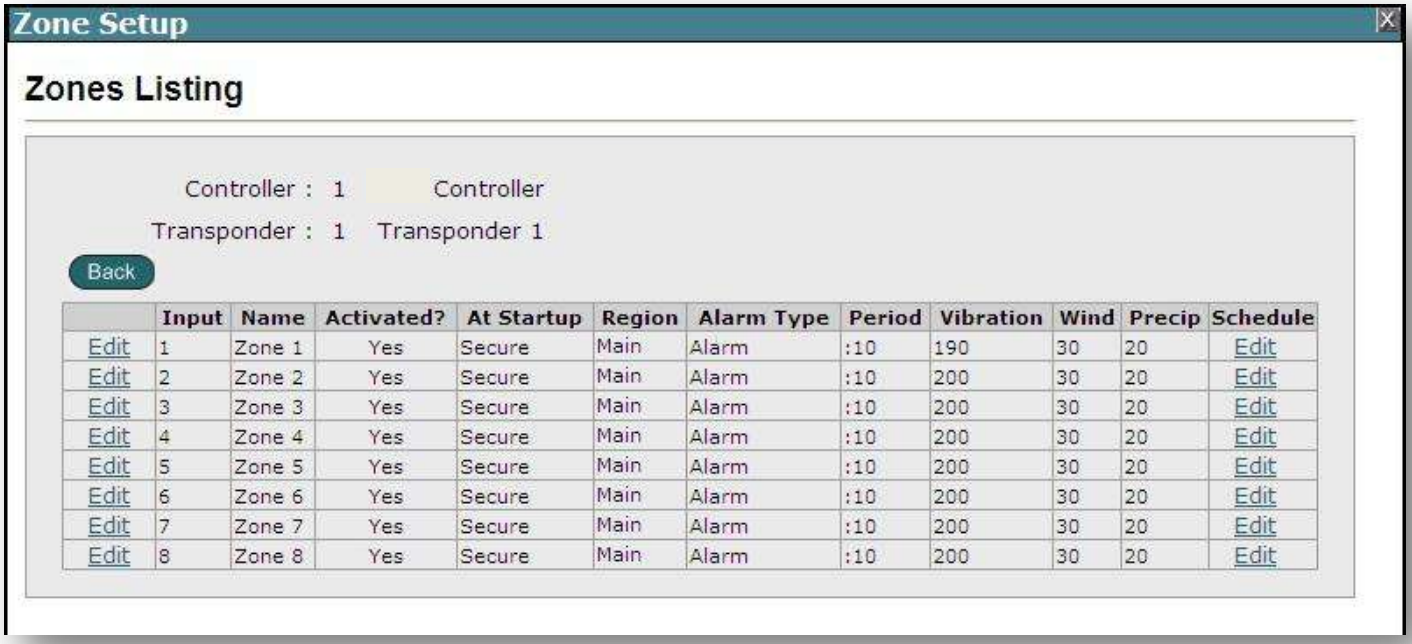


After this selection has been made the sites **Transponder Listing** will become available:

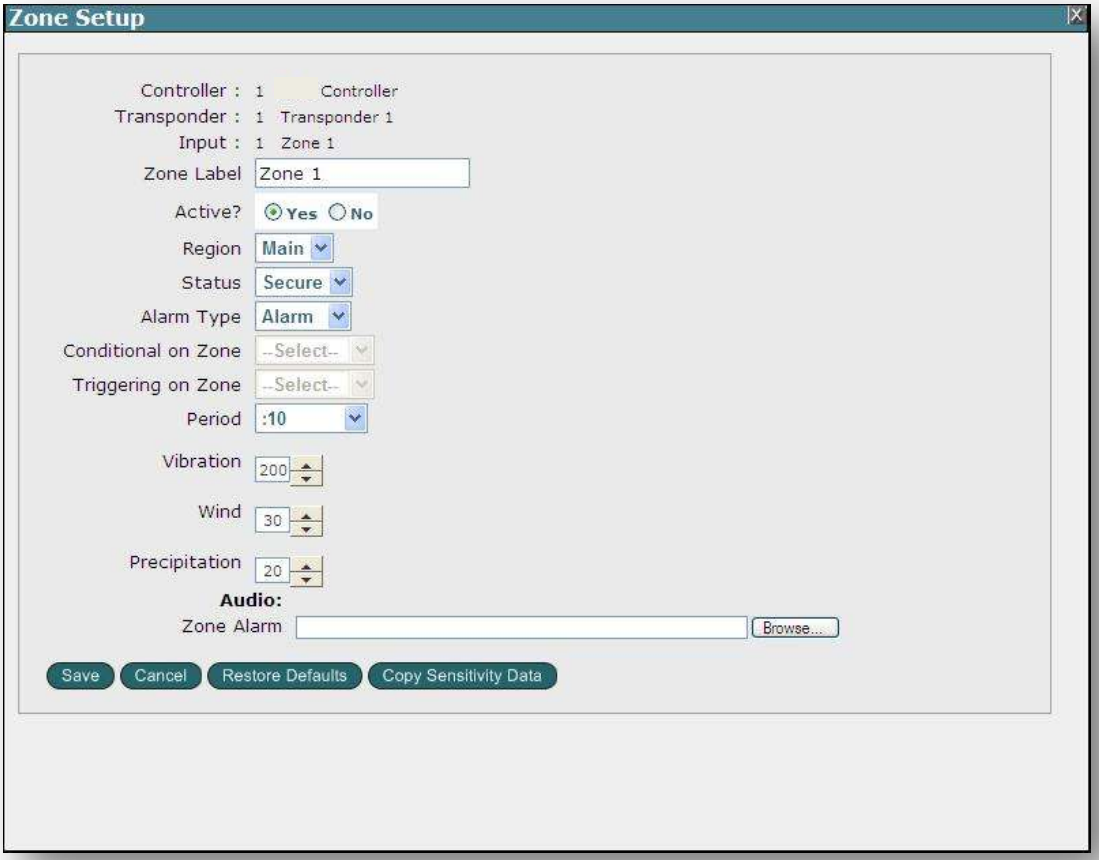


To view the current Zone parameters for Transponder 1 select the Edit under the **Zones** heading.

The **Zones Listing** for Transponder 1 is now available for review. To edit **Zone 1** zone parameters simply select the Edit to the left of the Input 1:

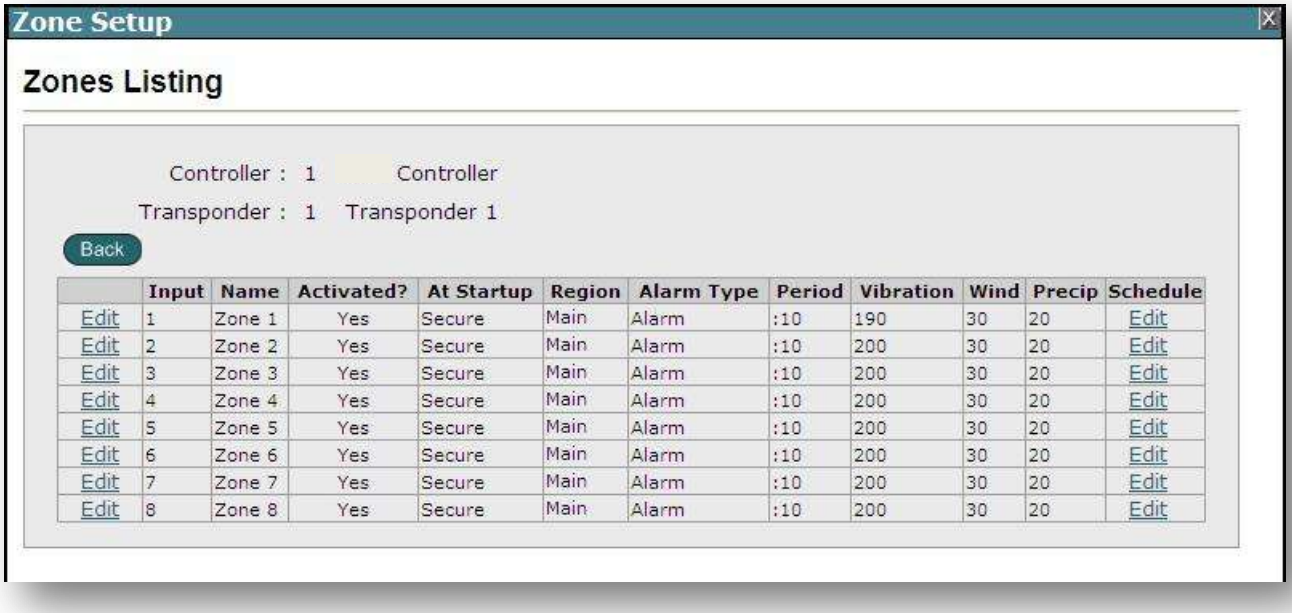

Zone Setup
Zones Listing
Controller : 1 Controller
Transponder : 1 Transponder 1
Back
Input
Name
Activated?
At Startup
Region
Alarm Type
Period
Vibration
Wind
Precip
Schedule
Edit 1 Zone 1 Yes Secure Main Alarm :10 190 30 20 Edit
Edit 2 Zone 2 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 3 Zone 3 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 4 Zone 4 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 5 Zone 5 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 6 Zone 6 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 7 Zone 7 Yes Secure Main Alarm :10 200 30 20 Edit
Edit 8 Zone 8 Yes Secure Main Alarm :10 200 30 20 Edit

This then displays its current zone settings:



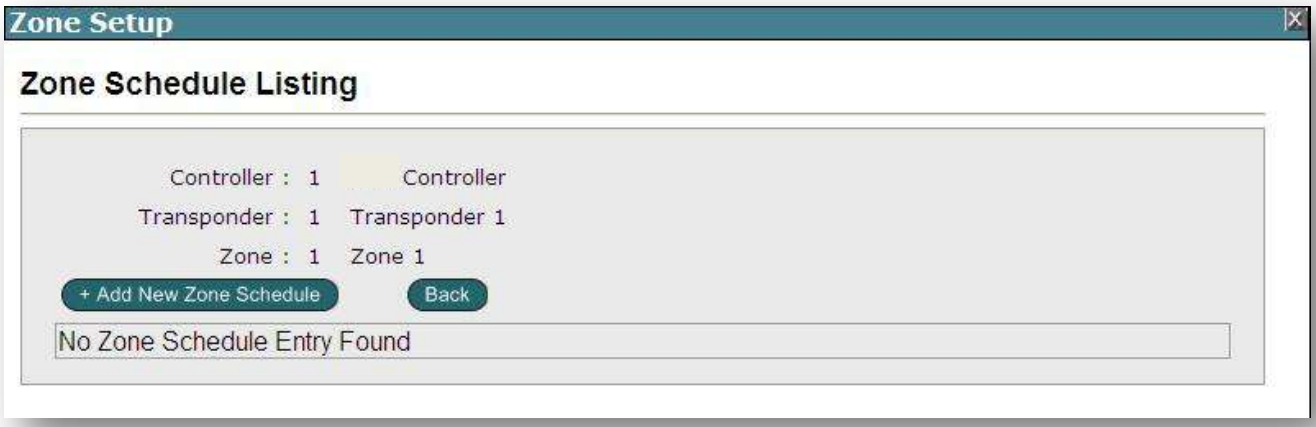
Scheduling Zone Status

There are times when site personnel may want to schedule zone status changes for authorized entry thereby eliminating nuisance alarms. To create a schedule for **Zone 1** select the Edit for this entry under the **Schedule** heading:



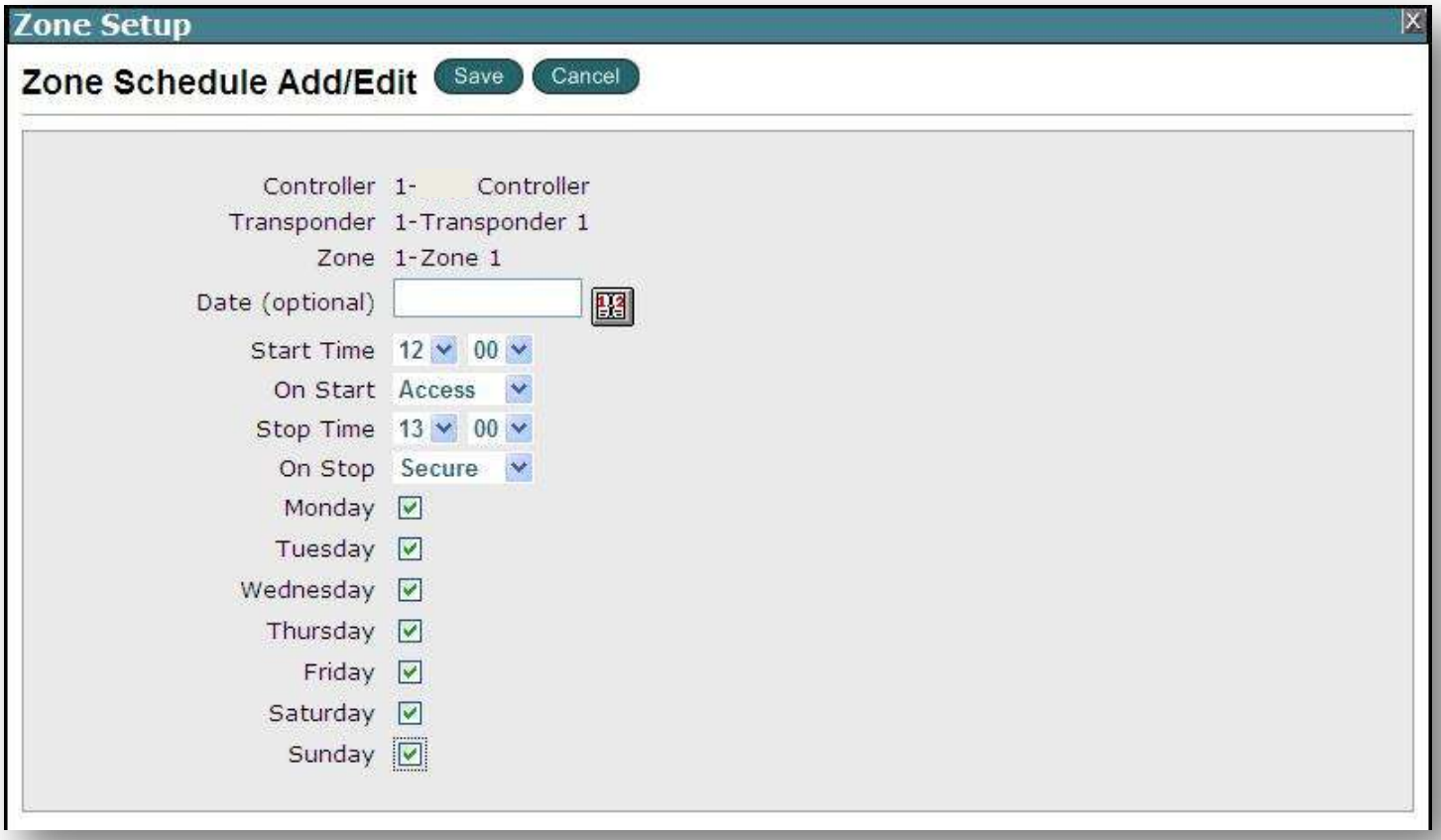
	Input	Name	Activated?	At Startup	Region	Alarm Type	Period	Vibration	Wind	Precip	Schedule
Edit	1	Zone 1	Yes	Secure	Main	Alarm	:10	190	30	20	Edit
Edit	2	Zone 2	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	3	Zone 3	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	4	Zone 4	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	5	Zone 5	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	6	Zone 6	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	7	Zone 7	Yes	Secure	Main	Alarm	:10	200	30	20	Edit
Edit	8	Zone 8	Yes	Secure	Main	Alarm	:10	200	30	20	Edit

The Zone Schedule Listing appears as follows:



Select **+ Add New Zone Schedule** since there are not currently any scheduled events for this Zone.

For this example site personnel have authorized deliveries daily from noon until 1 p.m. This is configured by entering the **Start Time**, status change **On Start**, **Stop Time**, status change **On Stop**, and days of the week. Note: for holidays or one day event schedules enter in the optional date. Valid status changes are **Secure, Access, and Disarm**. Select **Save** to complete the Zone Schedule Setup for that zone.



Section 4: System Notes and Reporting

Major points covered in this section:

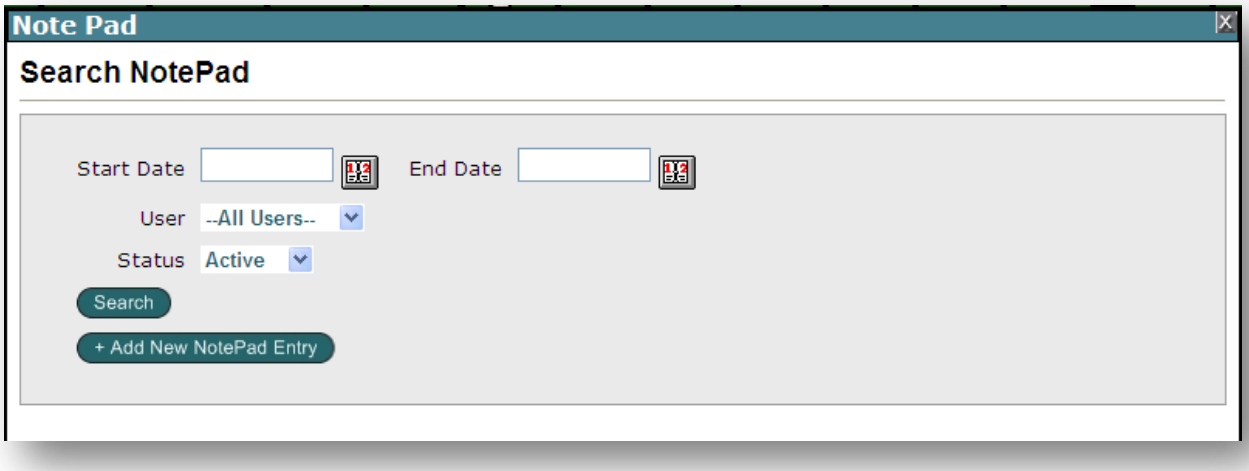
- ✓ Working with System Notes
- ✓ Configuring Standard Graphical Reports
- ✓ Using the Site Activity Report

Notes and Reporting Features

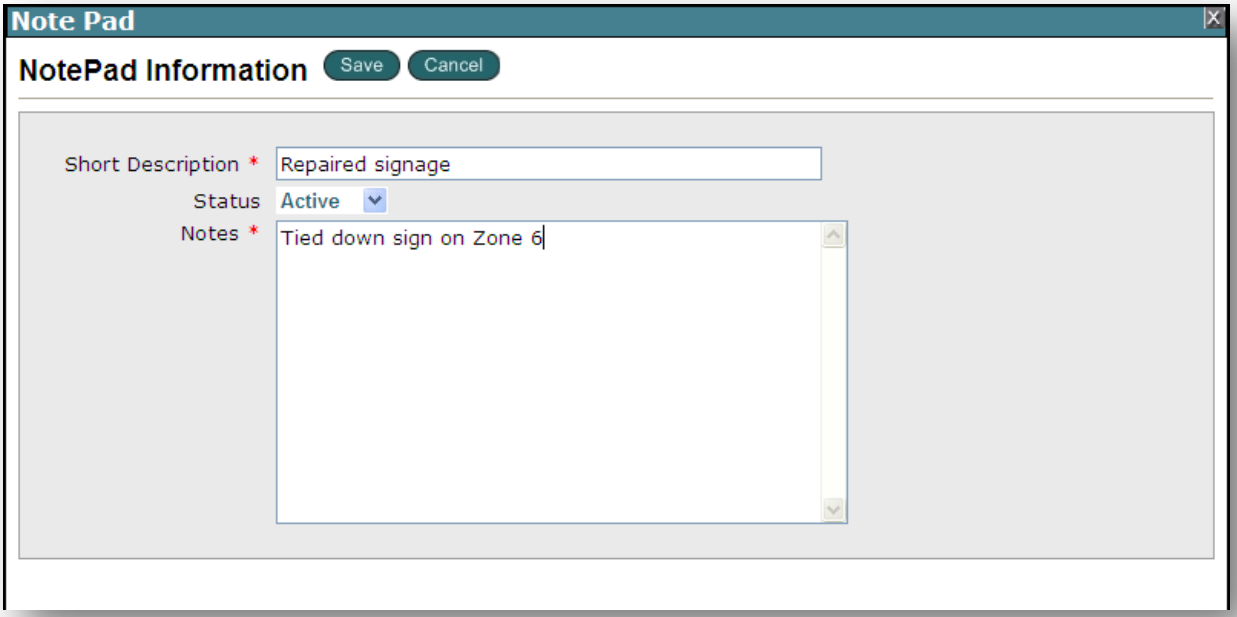
System Notes

Site personnel may need to document system issues for supervisors or relay information across shifts to track issues. Also notes may be added, or accessed later via a search by user and date for historical purposes. Simply locate and mouse click on the **Note Pad** sidebar menu item:

The Note Pad main window is presented allowing a search of existing system notes by **User**, **Date**, and **Status**. This is also the same interface to add to system notes. Notes are added by simply selecting **+ Add New Note Pad Entry**:



A **Short Description** and a large **Notes** field are available for a specific entry. Select **Save** to store the current system note. The Status field allows notes to be marked Inactive or Deleted if they are not relevant any longer.

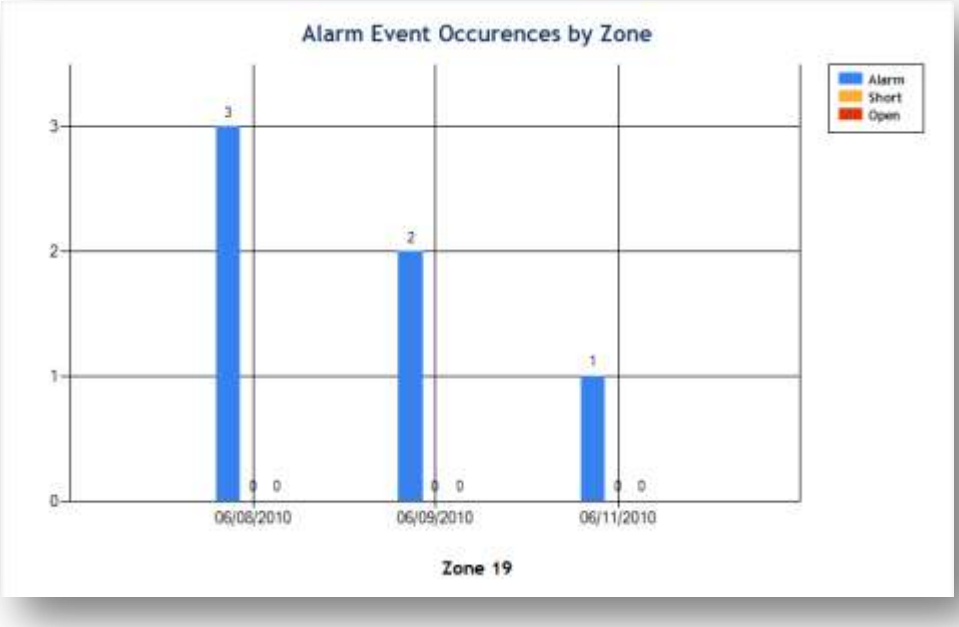


Standard Graphical Reports

Graphical Reports provide a quick, efficient method for alarm and site activity trending/analysis. The application provides five standard graphical reports:

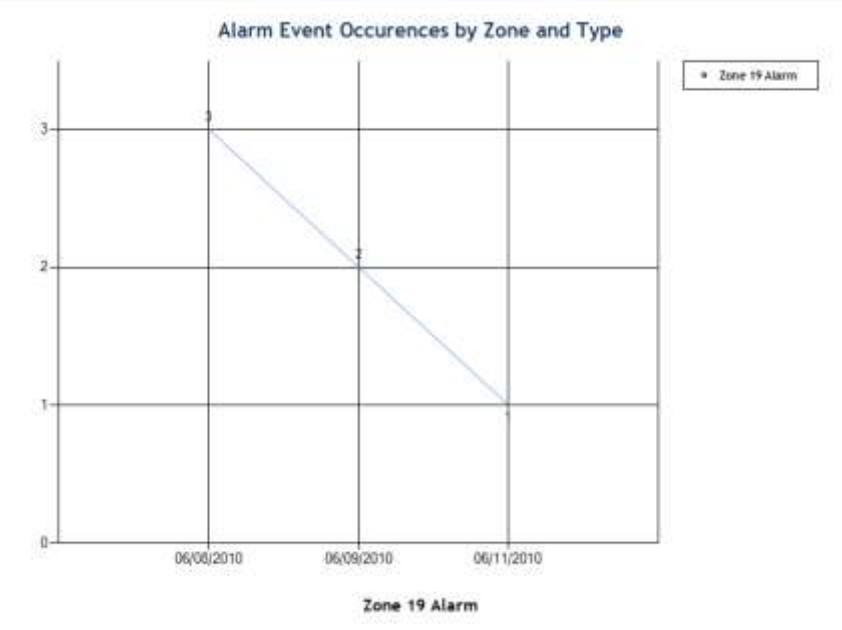
Alarm Event Occurrences by Zone

Bar Graph provides Alarm, Short, and Open event totals over a given period for a particular zone. This example graph illustrates a total of 6 Alarms over week period for Zone 19:



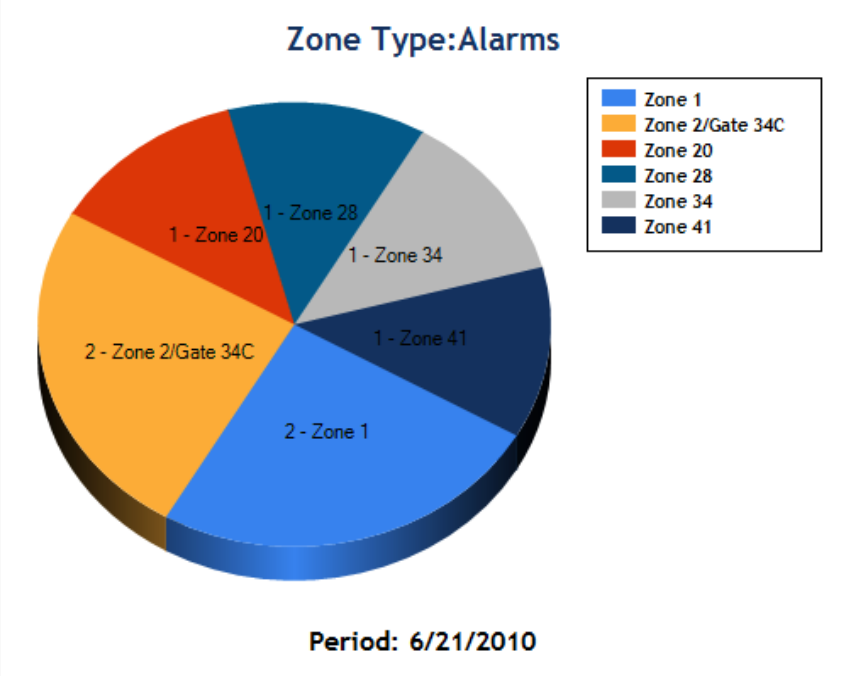
Alarm Event Occurences by Zone and Type

Line Graph provides Alarm or Short or Open event totals over a given period for a particular zone.
This example graph illustrates a total of 6 Alarms over week period for Zone 19:



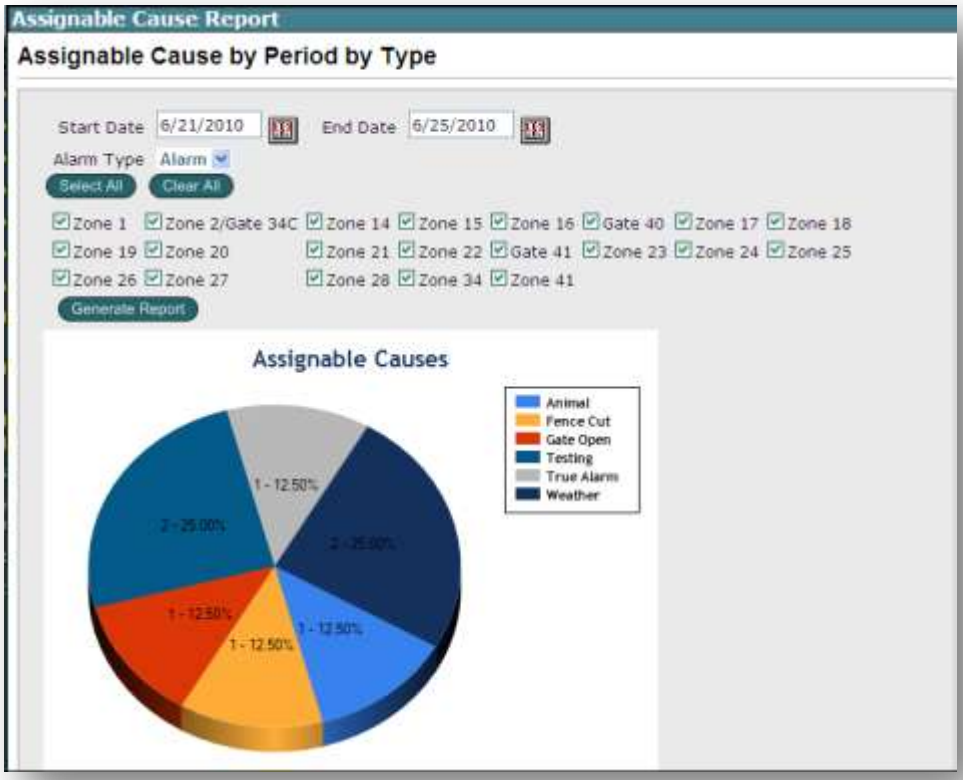
Alarm Frequency by Period and Type

Pie Chart provides Alarm frequency by type (Alarm, Short, or Open) by date.
This example graph reveals a breakdown of the Alarms reported on 6/21/2010 and their frequency:



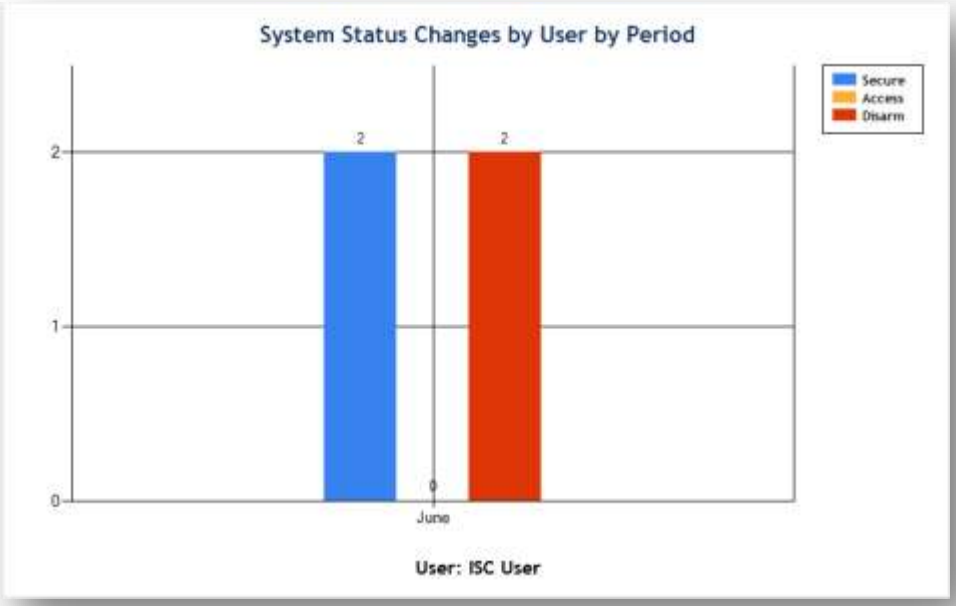
Assignable Cause Report

Pie Chart provides Assignable Cause distribution of one or more zones by period.
This example graph shows the breakdown of Assignable Causes for all Alarms reported on 6/21 through 6/25.


Assignable Cause Report
Assignable Cause by Period by Type
Start Date 6/21/2010
End Date 6/25/2010
Alarm Type Alarm
Select All
Clear All
Zone 1 Zone 2/Gate 34C Zone 14 Zone 15 Zone 16 Gate 40 Zone 17 Zone 18
Zone 19 Zone 20 Zone 21 Zone 22 Gate 41 Zone 23 Zone 24 Zone 25
Zone 26 Zone 27 Zone 28 Zone 34 Zone 41
Generate Report
Assignable Causes
Animal
Fence Cut
Gate Open
Testing
True Alarm
Weather
1 - 12.50%
2 - 25.00%
1 - 12.50%
1 - 12.50%
1 - 12.50%
2 - 25.00%

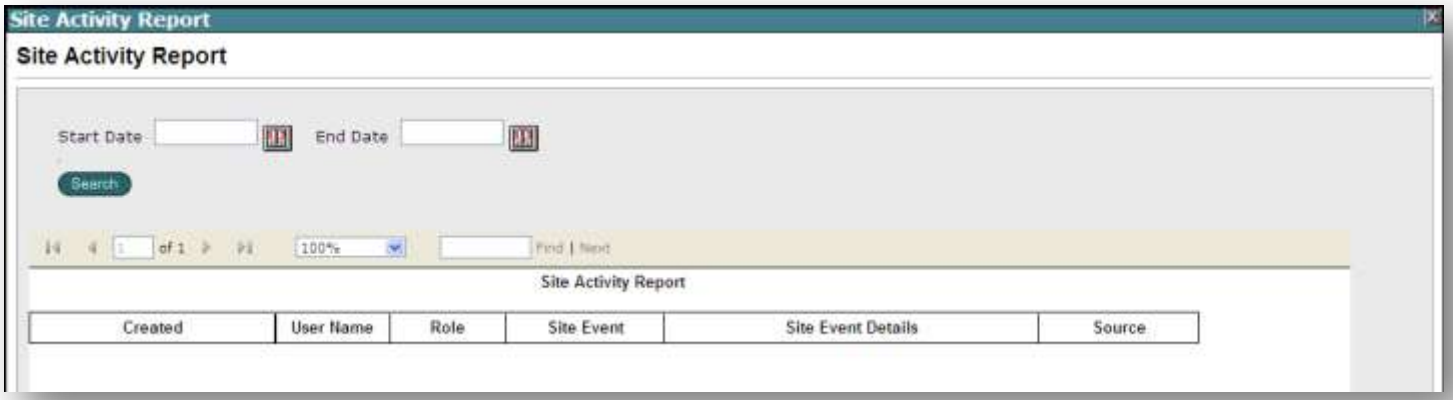
System Status Changes by User and Period

Bar graph provides System Status changes by User by Period.
This example graph shows the breakdown of Status Changes by ISC User.



Site Activity Report

All alarm reporting and system status information is written to a local database on the application's computer. This information can be retrieved via the **Site Activity Report**. The events are date and time stamped for analysis and period filtering. The reports can also be **Printed** to an **Adobe .pdf** format or **Exported** to **Microsoft .xls** format. When the menu option for the Site Activity Report is selected the user is prompted for **Start** and **End Dates**. The report is then generated by mouse clicking on the **Search** button (if Search is selected without dates entered all event records are provided).

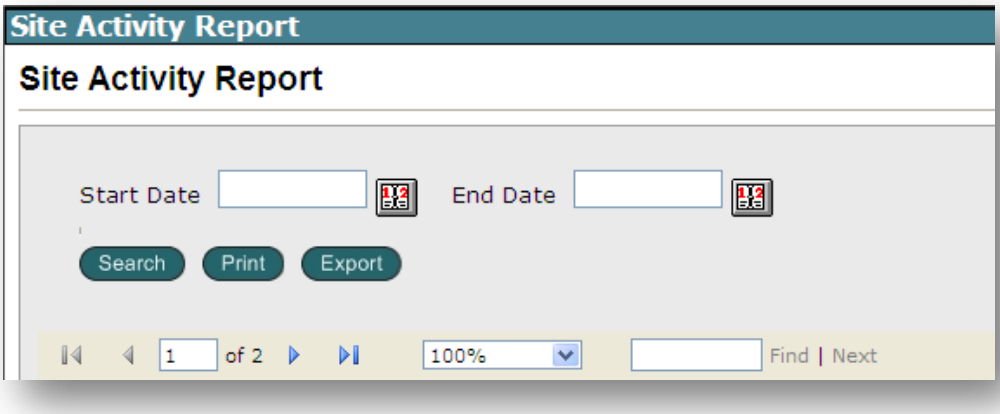


Here is an example Site Activity Report:

Site Activity Report

Created	User Name	Role	Site Event	Site Event Details	Source
8/10/2010 10:15:22 AM	master	Developer	Alarm - Clear	NRO Controller - Transponder 1 - Transponder Communication Notice - Clear - Testing, W=0, R=0	GUI
8/10/2010 10:15:13 AM	master	Developer	Alarm - Acknowledge	NRO Controller - Transponder 1 - Transponder Communication Notice - Acknowledge, W=0, R=0	GUI
8/10/2010 10:14:53 AM	master	Developer	User Logged In	User Logged in	GUI
8/10/2010 10:10:58 AM	master	Developer	Alarm - Acknowledge	NRO Controller - Transponder 1 - Transponder Communication Notice - Acknowledge, W=0, R=0	GUI
8/10/2010 10:09:53 AM	master	Developer	Alarm	NRO Controller - Transponder 1 - Transponder Communication Notice, W=0, R=0	ALARM SERVICE
8/10/2010 10:08:15 AM	master	Developer	Alarm - Clear	Zone 2 - Alarm Perimeter Fence - Clear - Testing, W=0, R=0	GUI
8/10/2010 10:06:33 AM	master	Developer	Alarm - Acknowledge	Zone 2 - Alarm Perimeter Fence - Acknowledge, W=0, R=0	GUI
8/10/2010 10:06:28 AM	master	Developer	Alarm	Zone 2 - Alarm Perimeter Fence - New, W=0, R=0	ALARM SERVICE
8/10/2010 10:06:20 AM	master	Developer	Alarm - Clear	Zone 2 - Alarm Perimeter Fence - Clear - Testing, W=0, R=0	GUI
8/10/2010 10:06:16 AM	master	Developer	Alarm - Acknowledge	Zone 2 - Alarm Perimeter Fence - Acknowledge, W=0, R=0	GUI
8/10/2010 10:06:16 AM	master	Developer	Alarm - Clear	Zone 1 - Alarm Perimeter Fence - Clear - Weather, W=0, R=0	GUI
8/10/2010 10:06:12 AM	master	Developer	Alarm - Acknowledge	Zone 1 - Alarm Perimeter Fence - Acknowledge, W=0, R=0	GUI
8/10/2010 10:06:08 AM	master	Developer	Alarm	Zone 2 - Alarm Perimeter Fence - New, W=0, R=0	ALARM SERVICE
8/10/2010 10:06:08 AM	master	Developer	Alarm	Zone 1 - Alarm Perimeter Fence - New, W=0, R=0	ALARM SERVICE
8/10/2010 10:04:57 AM	master	Developer	Alarm - Clear	NRO Controller - Transponder 1 - Transponder Communication Notice - Clear - Testing, W=0, R=0	GUI
8/10/2010 10:04:53 AM	master	Developer	Alarm - Acknowledge	NRO Controller - Transponder 1 - Transponder Communication Notice - Acknowledge, W=0, R=0	GUI
8/10/2010 10:04:02 AM	master	Developer	Alarm - Acknowledge	NRO Controller - Transponder 1 - Transponder Communication Notice - Acknowledge, W=0, R=0	GUI
8/10/2010 10:02:09 AM	master	Developer	Alarm	NRO Controller - Transponder 1 - Transponder Communication Notice, W=0, R=0	ALARM SERVICE
8/10/2010 10:01:11 AM	master	Developer	Alarm - Clear	Zone 2 - Alarm Perimeter Fence - Clear - Testing, W=0, R=0	GUI
8/10/2010 10:01:08 AM	master	Developer	Alarm - Acknowledge	Zone 2 - Alarm Perimeter Fence - Acknowledge, W=0, R=0	GUI
8/10/2010 9:59:17 AM	master	Developer	Alarm	Zone 2 - Alarm Perimeter Fence - New, W=0, R=0	ALARM SERVICE

The Site Activity Report can be saved electronically to be printed at a later date or exported to a spreadsheet for additional sorting and analysis.



Printing Site Activity Reports

Selecting the **Print** button saves the **Site Activity Report** to a Portable Document File (.pdf). This file is automatically saved to the path C:\Inetpub\wwwroot\ISCGUI\Web\Print and named **SiteActivity** followed by the date and time it was generated. A shortcut is available on the Desktop for ease of access.

Exporting Site Activity Reports

Selecting the **Export** button saves the **Site Activity Report** to a Microsoft Excel Spreadsheet (.xls). This file is automatically saved to the path C:\Inetpub\wwwroot\ISCGUI\Web\Export and named **SiteActivity** followed by the date and time it was generated. A shortcut is available on the Desktop for ease of access.